ACTUALITÉS EUROPÉENNES

21 juillet 2016

Commission des affaires européennes

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Après quatre années de négociations, le règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE, a officiellement été publié, le 27 avril 2016, au Journal officiel de l'Union européenne.

Le règlement vise à concilier deux objectifs : renforcer le droit des citoyens de l'Union et responsabiliser les différents acteurs du traitement des données. Il entrera en vigueur en mai 2018.

Le renforcement des droits des citoyens de l'Union européenne

La protection des données à caractère personnel et le respect de la vie privée sont des droits fondamentaux majeurs consacrés par les traités. Toute utilisation d'informations, concernant une personne physique identifiée ou identifiable, doit être soumise au respect d'un nouveau cadre général de protection issu du règlement.

L'objectif essentiel est de **renforcer l'information des citoyens** à travers des exigences relatives à la **transparence de l'information** et également aux **finalités** recherchées par l'information. Ainsi, en plus des caractères « *concis, transparent, intelligible et facile d'accès* » attachés à l'information, cette dernière doit permettre à la personne concernée d'être informée de l'existence du traitement des données ou de la durée probable pendant laquelle elles seront conservées.

Toutefois, pour que l'information circule, le **consentement de la personne concernée est absolument nécessaire.** Afin d'empêcher l'utilisation abusive des données, le règlement encadre leur utilisation à travers deux exigences précises : d'une part, il consacre le droit de la personne à donner et retirer son consentement et, d'autre part, il attribue des caractères au consentement. Ainsi, le traitement des données ne peut se faire sans le consentement de la personne concernée et uniquement à des fins déterminées jusqu'au moment où la personne décide de retirer son consentement. Ce dernier doit être « **indubitable** » pour les traitements de données sensibles et « **explicite** » dans tous les cas où il est exigé.

Les étapes du règlement européen sur la protection des données personnelles

- 25 janvier 2012, Commission européenne : publication de la proposition de règlement général sur la protection des données personnelles ;
- 4 mars 2012, Sénat : adoption d'une résolution européenne portant avis motivé sur la protection des données personnelles au titre du contrôle du principe de subsidiarité ;
- 6 mars 2012, Sénat : adoption d'une résolution européenne sur la protection des personnes physiques à l'égard des données personnelles ;
- 12 mars 2013, Sénat : adoption d'une résolution européenne sur le transfert des données à caractère personnel en matière pénale par les autorités judiciaires et policières ;
- 12 mars 2014, Parlement européen : soutien et vote de la proposition de réforme de la protection des données présentée par la Commission européenne ;
- 15 juin 2015, Conseil de l'Union européenne : accord scellé par les ministres de la justice de l'UE réunis au sein du Conseil « Justice » sur l'orientation générale du Conseil concernant la proposition de règlement général sur la protection des données présentée par la Commission européenne ;
- 24 juin 2015, Trilogue entre la Commission européenne, le Parlement européen et le Conseil de l'Union européenne : consensus sur un accord final ;
- 17 décembre 2015, Commission LIBE du Parlement Européen, le Coreper et la Commission européenne : consensus et adoption des textes ;
- 14 avril 2016 : adoption du règlement par le Parlement européen en plénière ;
- 2018 : application du règlement.

À côté des droits – d'accès, de rectification ou d'opposition – existants, le règlement consacre plusieurs autres droits. Ainsi, un **droit à l'effacement des données**, dit « droit à l'oubli », est consacré. Ce droit permet à la personne concernée d'obtenir du tiers l'effacement de tous les liens vers les données à caractère personnel diffusées qu'un tribunal ou une autorité réglementaire a jugé nécessaire. Le responsable du traitement devra alors prendre toutes les mesures raisonnables pour procéder à l'effacement de ces données, y compris par des tiers. Toutefois, certaines **exceptions au droit à l'oubli** sont prévues si le traitement de ces données est justifié pour exercer le droit à la liberté d'expression et d'information, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins d'archivage dans l'intérêt général ou à des fins scientifiques, statistiques et historiques.

En outre, le règlement a souhaité garantir un **droit à la limitation du traitement** ainsi qu'un **droit à la portabilité**, facilitant le transfert de données à caractère personnel d'un fournisseur de services à un autre, et surtout, il encadre désormais le « *profilage* » en permettant aux personnes de s'opposer aux traitements aboutissant à une décision automatisée et susceptibles de porter atteinte à leurs droits.

Enfin, le règlement prévoit une **protection spécifique des mineurs**. En effet, entre 13 et 16 ans selon les États, le consentement des parents est requis pour procéder au traitement des données. Cette protection s'est révélée nécessaire au regard du nombre croissant de mineurs utilisant les réseaux sociaux.

Toutefois, le texte prévoit des **exceptions aux règles générales** pour les traitements de données journalistiques, l'accès aux documents officiels, l'utilisation du numéro national d'identification et les traitements effectués dans le cadre des relations de travail.

La contribution de la Cour de justice de l'Union européenne à l'évolution des règles relatives à la protection des données à caractère personnel

- **CJUE, 8 avril 2014, arrêt Digital Rights Ireland et Seitlinger e.a**. : la Cour de justice a invalidé la directive sur la rétention des données télécoms qui imposait aux opérateurs de télécommunication de stocker pour une durée minimale de six mois et maximale de deux ans les données de téléphonie des utilisateurs, afin qu'elles puissent être utilisées par les services répressifs des États membres dans la conduite d'enquête relatives à des infractions graves. La Cour a considéré que les mesures prévues par cette directive n'étaient pas accompagnées des garde-fous nécessaires.
- **CJUE, 13 mai 2014, arrêt Google Spain c./ AEPD** : la Cour de justice a jugé que toute personne a, sous certaines conditions, un droit au déréférencement des informations la concernant. Elle considère que l'exploitant d'un moteur de recherche peut être tenu responsable du traitement de données personnelles figurant sur des pages web publiées par des tiers, et que, à ce titre, les personnes concernées peuvent demander à ce que les liens menant vers ces données soient supprimés lorsqu'elles ne sont plus actuelles ou pertinentes. La personne concernée peut donc s'adresser directement à l'exploitant pour obtenir la suppression d'un lien de la liste de résultats, et le moteur de recherche peut y être contraint par les autorités compétentes de protection des données. Ce droit au déréférencement n'est toutefois pas absolu, et la suppression de ces liens doit être appréciée au cas par cas.
- **CJUE, 6 octobre 2015, arrêt Schrems c./ Data Protection Commissionner** : la Cour de justice a invalidé la décision d'adéquation *Safe Harbor*, (« sphère de sécurité »), adoptée par l'Union européenne dans le cadre de la directive européenne de 1995 sur la protection des données qui permet l'échange de données entre entreprises de l'Union européenne et entreprises américaines respectant un certain niveau de protection des données. La Cour a considéré que ce mécanisme ne permettait pas d'assurer un niveau de protection suffisant des données à caractère personnel européennes transférées.

La responsabilisation des acteurs du traitement des données

Le règlement prévoit de nouveaux outils permettant d'accentuer la responsabilité et l'autonomie des responsables du traitement et ainsi garantir le respect absolu des nouvelles règles en matière de protection des données. Il s'agit d'un **modèle de contrôle et de sanction *a posteriori*,** puisque les entreprises pourront bénéficier d'une plus grande souplesse concernant la gestion des données à caractère personnel, mais elles seront susceptibles d'être sanctionnées plus lourdement.

La première mesure de responsabilisation consiste à **supprimer l'obligation de déclaration préalable** à la mise en œuvre d'un traitement automatisé des

données personnelles. Cette dernière est remplacée par **l'obligation de tenir une documentation** permettant aux responsables du traitement, des entreprises de plus de 250 salariés, de prouver leur conformité au texte. Les entreprises de moins de 250 salariés, qui réalisent des traitements de données occasionnels, sont dispensées de l'obligation de tenir un registre des traitements.

L'objectif est double : responsabiliser et réduire les coûts administratifs à travers deux nouveaux systèmes.

Tout d'abord, le nouveau principe de responsabilité est fondé sur **un système d'analyse de risques** à réaliser en interne. Cela oblige le responsable, par le biais d'une analyse d'impact et pour les traitements jugés potentiellement risqués au regard des droits et des libertés, de consulter son autorité de référence avant de le mettre en œuvre. Cette autorité de protection des données (en France, la Commission nationale de l'informatique et des libertés, la CNIL) pourra lui imposer des mesures à mettre en place en son sein afin de respecter les dispositions légales. Ainsi, en fonction des résultats de l'analyse des risques, le responsable du traitement pourra être amené à **désigner un Délégué à la protection des données (ci-après DPO).** Ce dernier, dont la désignation s'impose aux autorités publiques et à certaines entreprises, sert de point de contact aux contrôleurs et participe aux analyses d'impact (obligatoires pour le « *profilage* » et la surveillance des personnes à grande échelle).

D'autre part, dans des affaires transfrontières importantes faisant intervenir plusieurs autorités de contrôle nationales, une décision de contrôle unique sera prise. C'est le **mécanisme du « guichet unique »** (« *one-stop-shop* ») qui permet à une entreprise ayant des filiales dans plusieurs États membres de n'avoir à traiter qu'avec l'autorité de contrôle de l'État membre dans lequel elle a son établissement principal. L'autorité de contrôle agit alors à titre d'« *autorité de contrôle chef de file* », et en cas de désaccord, le Comité européen de la protection des données (« *European Data Protection Board* », EDPB) sera consulté. Ce dernier remplace l'actuel groupe de travail G29 et permet d'assurer une application cohérente du règlement au sein des différents États membres en rendant des avis contraignants et en arbitrant les différends entre les autorités.

Pour veiller à ce que le règlement résiste à l'épreuve du temps, les principes de la protection des données **dès la conception** (« *Privacy by design* ») et de la protection des données **par défaut** (« *Privacy by default* ») sont introduits. Les responsables de traitement devront garantir que les traitements de données ne portent pas atteinte à la vie privée des personnes au moment de la conception du traitement mais également tout au long de la durée de vie du traitement à l'aide d'un processus d'audit préalablement défini.

Enfin, le règlement prévoit des mesures de sécurité que les responsables du traitement devront mettre en œuvre, avec l'obligation dans certains cas de notifier les violations de données à caractère personnel. Le règlement entérine ainsi **l'obligation de notification des fuites de données** aux autorités dans un **délai de 72 heures.**

Afin de conseiller et d'orienter les entreprises dans leur mise en œuvre des nouvelles règles, des **codes de conduites** par secteur d'activité et des **certifications** proposés par le CEPD et les institutions de l'Union permettront d'attester de la conformité au règlement des traitements effectués par une entreprise.

©AP Images/European Union – EP

Aujourd'hui, la responsabilisation des acteurs a des conséquences concrètes pour les personnes concernées qui jouissent d'un **droit à réparation du préjudice subi**. Ainsi, elles peuvent introduire une **réclamation auprès d'une autorité de contrôle ou former un recours juridictionnel,** qui peut être effectué parallèlement au dépôt d'une plainte auprès de la CNIL. Deux seuils sont fixés pour les sanctions en cas de non-conformité au règlement, qui varient selon la nature de l'infraction : pour les infractions mineures, le seuil est fixé à 2 % du chiffre d'affaires mondial ou 10 millions d'euros pour les infractions mineures ; pour les infractions les plus graves, le seuil est fixé à 4 % du chiffre d'affaires mondial ou 20 millions d'euros.

Enfin, des nouvelles règles concernant le **transfert de données vers les pays tiers et les organisations**

internationales hors Union européenne sont prévues par le règlement et prévoient la possibilité de se fonder sur un **code de conduite** (« *Binding Corporate Rules* ») **par secteur d'activité** contribuant à l'application du règlement ou sur un label. Le règlement affirme par ailleurs expressément qu'un transfert hors Union ne peut être imposé par les lois et règlements d'un pays tiers à l'Union et que les transferts peuvent intervenir à condition que différentes conditions et garanties soient respectées, en particulier lorsque la Commission a décidé qu'un niveau adéquat de protection existe. Ainsi, le transfert des données vers des États tiers ne nécessitera plus d'autorisation de transfert par la CNIL mais exigera la signature d'un contrat de transfert de données. Ces nouvelles dispositions devront nécessairement être prises en considération par l'accord – en cours de négociation avec les États-Unis – **« *Privacy Shield* »** (« bouclier de confidentialité »).

Le paquet sur la protection des données personnelles inclut par ailleurs une **directive relative aux transferts de données à des fins policières et judiciaires,** adoptée par le Parlement européen le 14 avril 2016. En effet, la nature particulière des activités policières et judiciaires requiert l'application de règles distinctes en matière de protection des données permettant de faciliter la libre circulation des données et de promouvoir la coopération entre les États membres. La directive s'applique aux transferts de données à travers les frontières de l'Union européenne et fixe, pour la première fois, des normes minimales pour le traitement des données à des fins policières au sein de chaque État membre.

À l'instar du règlement, la directive prévoit un ensemble de **principes permettant de protéger les individus**, qu'il s'agisse de la victime, du criminel ou du témoin, en prévoyant des droits et des restrictions clairs en matière de transfert de données **à chaque étape du procès pénal** (enquête, poursuites pénales, jugement) et dans la phase de l'exécution des peines. Elle décrit également les compétences du responsable du traitement en incluant des garanties et des mesures de prévention sur les menaces à la sécurité publique. Si la directive permet de faciliter la coopération entre les autorités répressives, elle consacre parallèlement l'existence d'autorités de contrôle et la possibilité d'obtenir réparation notamment lorsque les données sont transférées vers un pays tiers à des fins répressives alors même que ce dernier n'assure pas un niveau de protection adéquat.

Les démarches à suivre par les entreprises

Analyser
- Identifier les contrats existants dans lesquels les acteurs sont responsables du traitement des données ;
- Consulter l'autorité de référence avant de mettre en œuvre le traitement.

Désigner
- Désigner un Délégué à la protection des données (DPO) ;
- Désigner un représentant en France si l'entreprise est établie en dehors de l'Union européenne et met en œuvre des traitements sur le territoire français.

Contrôler
- Réaliser un audit des traitements de données à caractère personnel ;
- Réaliser une analyse d'impact pour les traitements jugés risqués au regard des droits et des libertés.

Veiller
- Mettre en place des mesures techniques et organisationnelles appropriées (« *accountability* ») ;
- Tenir une documentation permettant de démontrer le respect des principes ;
- Intégrer les principes de la protection des données dès la conception (« *Privacy by design* ») et par défaut (« *Privacy by default* ») pour l'ensemble des projets.